--DRAFT--

REMARKS

Applicants respectfully request favorable reconsideration of this application, as amended.

Claims 19, 21, 23-36 and 39 are pending. By this amendment, Claims 19, 33, and 39 have been amended to more particularly recite subject matter which Applicants regard as their invention, as discussed in detail below. Claims 1-18, 20, 22, 37-38, and 40 were previously cancelled without prejudice or disclaimer.

In the Office Action, claims 19, 21, 23-36 and 39 were rejected under 35 U.S.C § 103(a) over Hopkins in combination with Inada.

Without acceding to the rejection, Claim 19 has been amended to recite, *inter alia*, encryption means (B3) for producing an encrypted text (C), intended to be associated with said message (m), using said personalized data (z, Kz) of one said individual member (M) only, and signing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members using the message to be signed (m) and said encrypted text (C) produced using the personalized data (z, Kz) of said one individual member (M) only.

Support is provided at, for example, page 1, lines 9-13; and page 13, lines 22-24 of Applicants' disclosure. It is apparent that the applied references do not teach or suggest at least these features.

For example, the Office Action acknowledges at pages 3, 6, and 7 that the primary reference, Hopkins, does not teach or suggest these features. However, it is alleged that Hopkins deficiencies in this regard are cured by the teachings found in secondary reference Inada.

Secondary reference Inada, for its part, is directed to a group encryption/decryption method and apparatus. In Inada, a group signature is generated by an individual of a group on behalf of the group, by using a group private key. *See* Inada, col. 2, lines 39-43; col. 6 lines, 8-18; and col. 13, lines 22-37. Inada teaches that all the group members are thus using the same key to generate a group signature on behalf of the group. Inada, col. 6, lines 19-22; and col. 13, lines 22-37. Thus, Inada teaches the enabling of an individual of a group to generate individually a group signature on behalf of the group. However, Inada's method is understood as teaching that the same group private key must be used by the different members of the group. In other words, Inada's group private key is not a personalized data of an individual of the group. Thus, it is apparent that Inada does not teach or suggest encryption means (B3) for producing an encrypted text (C), intended to be associated with said message (m), using said personalized data (z, Kz) of said individual member (M) only, as recited in Claim 19.

Furthermore, the cited portion of Hopkins relied on by Office Action as allegedly teaching or suggesting Applicants' signing means (B6) for producing the group signature (S) with a private signature key (SK) clearly discloses that the key used by the individual to generate a partial signature in Hopkins is an individual private key, and that "[t]he partial digital signatures are then combined mathematically to create a group digital signature." *See* Hopkins, col. 5, lines 22-31; and col. 11, lines 40-55.

Hopkins further teaches that in his signing process using group private key D, "each of the members of each group has control over at least one of the prime factors

$p_1, p_2, \ldots p_k$, but wherein no single one of the individuals of the group controls all of the prime factors used by the entirety." Hopkins, col. 10, lines 11-19.

Thus, it is apparent that if Hopkins were somehow modified to accommodate Inada's teachings regarding a group private key which common to all members of the group (e.g., not personalized), the resulting structure would be rendered inoperative for Hopkins' purpose of no single one of the individuals of the group controlling all of the prime factors used for the group private key D. Therefore, Applicants respectfully submit that Hopkins and Inada are not properly combinable.

Still further, assuming *arguendo* that Hopkins means for producing a partial signature by each user could be somehow interpreted as Applicants' encryption means as recited in claim 19 for producing an encrypted text (e.g., a partial signature in Hopkins) by using a personalized data (e.g., the individual private key of each user in Hopkins), then Hopkins cannot be seen as teaching or suggesting that the group signature is produced using the message to be signed -- that is, not modified by the encryption means -- and the encrypted text, as Hopkins' group signature is generated only using the encrypted texts (e.g., partial signatures).

Accordingly, Applicants respectfully submit that neither Hopkins nor Inada, whether taken alone or in combination, teaches or suggests encryption means (B3) for producing an encrypted text (C), intended to be associated with said message (m), using said personalized data (z, Kz) of one said individual member (M) only, and signing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members using the message to be signed (m) and said encrypted text (C) produced using the personalized data (z, Kz) of said one individual member (M) only, as recited in Claim 19.

--DRAFT--

Therefore, Applicants respectfully submit that Claim 19 distinguishes patentably form the applied references.

In addition, Claim 33 recites, *inter alia*, producing the group signature (S) of the message (m) by signing, with a private signature key (SK) common to all group members, a set including the message (m) and encrypted text (C) produced using a personalized data (z, Kz) of said one individual member (M) only.

Further, Claim 39 also recites, *inter alia*, an electronic device configured to store a personalized data (z, Kz) identifying one said individual member (M) of the group (G), to produce an encrypted text (C) intended to be associated with said message (m) using said personalized data (z, Kz) of said one individual member (M), and to produce the group signature (S) with a private signature key (SK) common to all group members using the message (m) and said encrypted text (C) produced using the personalized data (z, Kz) of said one individual member (M) only, and to output the message (m) and the group signature (S).

Therefore, Applicants respectfully submit that Claims 33 and 39 also distinguish patentably from the applied reference for at least the reasons discussed above with respect to Claim 19.

The dependent Claims 21, 23-32, and 34-36 are also believed to be patentable based on their dependence from Claims 19 and 33, as well as due to the additional features recited in Claims 21, 23-32, and 34-36.

Therefore, Applicants respectfully submit that this application is in condition for allowance. A prompt Notice of Allowance is respectfully requested.

--DRAFT--

Should the Examiner believe that any further action is necessary to place this application in better form for allowance, the Examiner is invited to contact Applicants' representative at the telephone number listed below.

The Commissioner is hereby authorized to charge to Deposit Account No. 50-1165 (T2678-9156US01) any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

Date: _____

By: DRAFT
Eric G. King
Reg. No. 42,736

Miles & Stockbridge, P.C.
1751 Pinnacle Drive, Suite 500
McLean, Virginia 22102-3833
Telephone: (703) 610-8647
4852-4856-3971